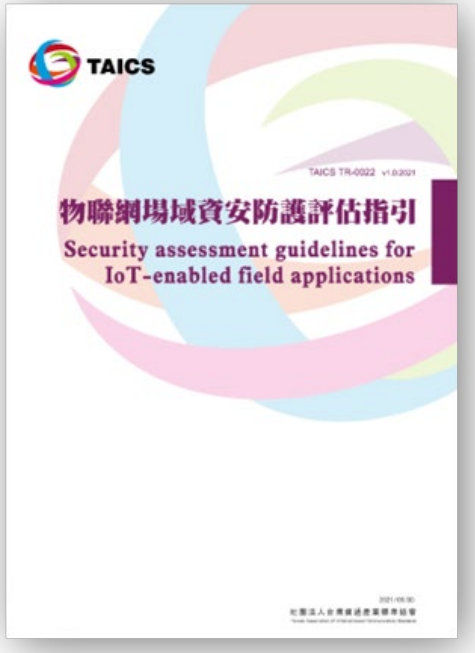
【徵案需求規格-計畫審查要項補充說明】

場域資安 & 5G基地臺軟體技術自主性

資訊安全規劃

- 資訊安全經費應占總經費至少7%
- 關鍵設備(如核心網路、基站、伺服器等)與應用服務系統，陸資企業或其產品或勞務不得參與。
- 提案廠商提案計畫場域之資訊安全，應符合台灣資通產業標準協會「**物聯網場域資安防護評估指引**」(編號TAICS TR-0022)，並至少取得L1評估標章，確保場域具備資安防護能力。



物聯網場域資安防護評估指引

提案計畫之場域必須依據台灣資通產業標準協會所公告之TAICS TR-0022「物聯網場域資安防護評估指引」進行威脅建模Threat Modeling、漏洞檢測Vulnerability Testing、滲透測試Penetration Testing及衝擊分析Impact Analysis等評測，確保場域具備資安防護能力。

物聯網場域資安防護評估指引

- (第1章) 適用範圍
- (第2章) 引用標準
- (第3章) 用語及定義
- (第4章) 資安防護評估

威脅建模 Threat Modeling（第5章）

1. 確認場域使用的軟硬體資產
2. 確認場域系統架構及應用情境(受保護的目標)
3. 確認場域系統資料流處理程序
4. 確認並記錄威脅
5. 評估威脅(損害, 可重製性, 入侵性,是否容易被發現...)

漏洞檢測 Vulnerability Testing（第6章）

1. 採用 CVSS通用漏洞評分系統評估資產設備漏洞風險等級
2. 針對物聯網系統進行靜態原始碼掃描
3. 制定滲透測試項目及評估惡意程式感染風險

滲透測試 Penetration Testing（第7章）

1. 參考OWASP IoT Top 10資安風險及已知各種場域可能的資安漏洞制定滲透測試規範
2. 根據威脅建模及漏洞檢測對應後制定滲透測試計畫

衝擊分析 Impact Analysis（第8章）

1. 依據滲透測試結果，評估IoT系統影響層面(包含技術、財務、人口、法律...)
2. 評估DREAD及OCTAVE Allegro兩種影響評估分析模型並依據不同垂直應用，選擇適當的評估方式

場域資安申請流程

申請表格撰寫

- 系統認證申請評估表：場域使用情境說明、佈署類型及地點、物聯網系統架構圖、物聯網系統網路拓樸圖(含資訊流)、安全控制項目自評表(含佐證資料)。
- 設備盤點清冊： 依照驗證場域實際建置狀況，填寫場域內Device、OS、Service、 Data、Flow、 Border、 Scenario及場域示意圖。
- 依審查內容持續修正至完稿。

漏洞修補及複測

- 依初測摘要進行漏洞修補。
- 完成漏洞修補後通知複測。

開案 — 2W — **填寫申請表** — 4~6W — **初測** — 3~4W — **複測** — 4W — **取證**

- 提供認證場域簡易情境說明、佈署類型、物聯網系統架構圖、網路拓樸圖，進行費用估算
- 回簽報價單正式開案。

- 確認場域100% Ready，並提供設備源碼掃描報告。
- 測試前務必完成設備盤點清冊，並確認軟硬體設備清單(含型號、設備IP、OS說明、版本等)、系統架構必須與實際環境相同。
- 受測方協助測試作業環境、待測設備準備、網路連線與故障排除。
- 進行威脅建模、漏洞/弱點檢測、滲透測試，產出初測摘要。

評估報告討論

提供OCTAVE Allegro影響程度評估，進行報告製作/衝擊分析與取證評估。

>4個月

(過案廠商)場域資安驗證應備申請文件

- **驗證單位開案證明(如報價單或委託單)**
- **系統認證申請評估表**，含申請者資料、場域使用情境說明、佈署類型及地點、安全控制項目自評表含佐證資料。
- **場域設備盤點清冊**，包括Device、OS、Service、Data、Flow、Border、Scenario等，場域建置PoC之相關資訊。

物聯網場域資安防護評估指引

系統認證申請評估表 (v4_20220325)

申請者公司名稱	:	XXX
統一編號	:	
營業所地址	:	
聯絡人	:	
聯絡人電話		
聯絡人電子郵件		
申請標章等級		
場域名稱	:	
場域位置	:	
申請日期	:	

系統認證申請評估表

Device

ID	名稱*	地點*	敘述*	屬性*	型號*	硬體版本	韌體版本	軟體版本	作業系統名稱	廠牌*	設備類型*	通訊媒介*	IP	MAC 位址	帳號	帳號規則	使用者權限	密碼
DE_1	一號攝影機	工廠大門	監看進出人流	自建	Q1798-LE	A1	10.9.4	v4.9.83	N/A	AXIS	感測層	RJ45	10.0.0.10	AA:BB:CC:DD:EE:FE	axisadmin	0800010000	Admin	axispasswd
DE_2	二號攝影機	辦公室大門	監看進出人流	自建	Q1798-LE	A1	10.9.4	4.9.84	N/A	AXIS	感測層	RJ45	10.0.0.20	AA:BB:CC:DD:EE:FF	axisadmin	0800010000	Admin	axispasswd
DE_3	PC	警衛室	即時監控攝影機畫面	自建	Z6 G4	N/A	3.6	N/A	WINDOWS11 @21H2_22000.526	HP	應用層	RJ45 RJ45 RJ45	10.0.1.30 10.0.0.100 10.0.0.200	AA:BB:CC:DD:EE:EE AA:BB:CC:DD:EE:CC AA:BB:CC:DD:EE:CC	pcadmin	0800010000	Admin	pcpasswd
DE_4	NAS	機房	儲存攝影機畫面	自建	DS1621xs+	B1	A2022-2	N/A	DSM@7.0.1	Synology	應用層	RJ45	10.0.0.250	AA:BB:CC:DD:EE:AA	nasadmin aaaa4444	0800040000	Admin User	naspasswd 12345678
DE_5	路由器	機房	處理網路封包	自建	891F	C2	10.2	N/A	IOS@15.4	Cisco	網路層	RJ45	10.0.0.253	AA:BB:CC:DD:EE:BB	N/A	0801010200	Admin	0801010200

OS

ID	名稱*	版本*	廠牌*	類型*	帳號	帳號規則	密碼	密碼規則	使用者權限	認證方式	金鑰位置	裝置ID*
OS_1	Windows11	21H2_22000.526	Microsoft	Normal	pcadmin	0800010000	pcpasswd	0800010000		使用者帳密	/usr/share/key	DE_3
OS_2	DSM	7.0.1	Synology	Normal	nasadmin aaaa4444	0800010000	naspass			使用者帳密		DE_4
OS_3	IOS	15.4	Cisco	Normal	N/A					使用者帳密		DE_5
OS_4	httpd	2.4.52	Apache	Virtual	w			0000	Admin	使用者帳密		DE_3
OS_5	mariadb	10.7.1	MariaDB	Container	dl		swd	0100000000	Admin	使用者帳密		DE_3

場域設備盤點清冊

Service

ID	名稱*	敘述*	類型*	IP*	Port*	協定*	帳號	帳號規則	密碼	密碼規則	使用者權限	認證方式	金鑰位置	包含套件*	服務版本	裝置ID*	作業系統ID
SE_1	影像串流	攝影機即時影像串流	遠端	10.0.0.10	554	RTSP@2.0	rtspaccount rtspuser	0800010000	rtsppasswd rtsp12345	0800010000	admin user	帳號密碼	N/A	RTSP-Dev@1.2 ssllib@2.0	2.0	DE_1	
SE_2	攝影機管理網頁	攝影機設定	遠端	10.0.0.20	8080	HTTP@1.1	aa 123	0100000000	aa 456	0100000000	admin user	帳號密碼	N/A	httpd@3.1		DE_2	

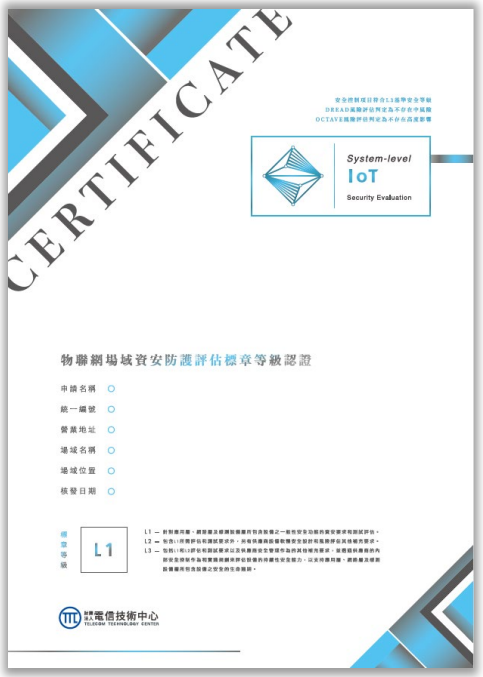
過案廠商申請注意事項

- 為配合驗收，建議過案廠商至少於驗收前4個月內完成場域PoC驗證，保留檢測(5~6週)及複測時程(原則上2週內，其時程仍視評估結果及建議調整) 。
- 過案廠商若委託資安輔導公司進行測試溝通，於申請驗證時應出具委任書(形式不拘)，避免正式測試時衍生爭議。
- 執行TAICS TR-0022時，過案廠商必須提供相關技術資訊，包含系統運作架構、資產設備名稱與用途、場域商業目標、使用需求情境和對應之系統功能、網路架構圖、設備間之資料流向和IP位址、登入設備之測試帳號密碼、管理權限及組態設定、設備操作介面說明、系統資料收集/處理/儲存的類型和做法、場域現有管控作為和防護機制等技術說明等，且必須密切配合檢測團隊。
- 基於誠信原則，所有資料應如實提供並不得造假，且場域範圍須與提案規劃相同，惟因審查委員或主管機關要求調整場域架構者，不在此限。

標章等級及核發要求

- L1：係指針對應用層、網路層及感測設備層所包含設備之一般性安全功能的資安要求和測試評估。
- L2：係指包含L1所需評估和測試要求外，另有供應商設備軟體安全設計和風險評 估其他補充要求。
- L3：包括L1和L2評估和測試要求以及供應商安全管理作為的其他補充要求。並透過供應商的內部安全控制作為和實踐規劃來評估設備的持續性安全能力，以支持應用層、網路層及感測設備層所包含設備之安全的生命週期。

標章等級	標章樣式	核發要求
L1	System-level IoT Security Evaluation	**① 安全控制項目須符合L1基準安全等級** **② DREAD風險評估判定為不存在高風險** **③ OCTAVE風險評估判定為不存在高度影響**
L2	System-level IoT Security Evaluation	① 安全控制項目須符合L2基準安全等級 ② DREAD風險評估判定為不存在中風險 ③ OCTAVE風險評估判定為不存在高度影響
L3	System-level IoT Security Evaluation	① 安全控制項目須符合L3基準安全等級 ② DREAD風險評估判定為不存在中風險 ③ OCTAVE風險評估判定為不存在高度影響



L1證書樣張

5G基地臺軟體技術自主性

- 申請補助之廠商應至少針對5G基地臺之通訊協議層(如PHY、MAC、RLC、PDCP、SDAP、RRC、SCTP、GTP等)、介面協定(如Uu、F1、E1、E2、N1、N2、Xn等)及網元管理系統(EMS)等各功能範圍，提出其中至少1項以上須透過軟體原始碼(Source Code)修改之參數，以利後續查驗其技術自主能力。
- 技術自主性查驗測試舉例如下:

  ① 針對通訊協議層及介面協定，增/刪指定的 Optional IE，並透過封包解析確認是否可自行完成。

  ② 修改基地台原始碼，印出過渡的參數並檢查是否正確，例如 C-RNTI。

  ③ 針對軟體在不同的佈署方式(如 MAC-PHY split、high PHY split 等)下進行開發及效能修改。

  ④ 針對元件(L2/L3)外部介面進行修改與調整介接不同平台(PHY)。

  ⑤ 可以任意修正EMS原始碼。

【技術自主性範例1】增/刪指定的 Optional IE

- ORAN 架構下，選擇E2介面協定(E2AP)增加一項Optional IE

前

檢視修改原始碼前，未有RIC Indication SN IE

```
// RIC Indication SN (Optional)
```

後

新增RIC Indication SN IE

```
// RIC Indication SN (Optional)
if(mode&0x01) {
    E2AP_SETUP_IE(pRICindicationIEs_RICindicationSN, RICindication_IEs_t,
        ProtocolIE_ID_id_RICindicationSN, Criticality_reject, RICindication_IEs__value_PR_RICindicationSN);
    pRICindicationIEs_RICindicationSN->value.choice.RICindicationSN = subAct->indicationSn;

    ASN_SEQUENCE_ADD(dstPtr, pRICindicationIEs_RICindicationSN);
}
```

Wireshark · Packet 38 · any

```
▸ Frame 38: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Stream Control Transmission Protocol, Src Port: 35239 (35239), Dst Port: 38482 (38482)
▾ E2 Application Protocol
  ▸ Message Type: Indication (0x0005)
  ▸ RICrequestID
    RANfunctionID: 44
    RICactionID: 1
  ▸ IE: RICindicationType (28)
  ▸ IE: RICindicationHeader (25)
  ▸ IE: RICindicationMessage (26)
```

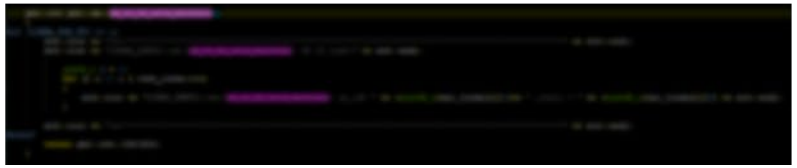
Wireshark · Packet 702 · any

```
▸ Frame 702: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Stream Control Transmission Protocol, Src Port: 38130 (38130), Dst Port: 38482 (38482)
▾ E2 Application Protocol
  ▸ Message Type: Indication (0x0005)
  ▸ RICrequestID
    RANfunctionID: 44
    RICactionID: 1
    RICindicationSN: 29
  ▸ IE: RICindicationHeader (25)
  ▸ IE: RICindicationMessage (26)
```

由Wireshark看出新增
RIC Indication SN欄位

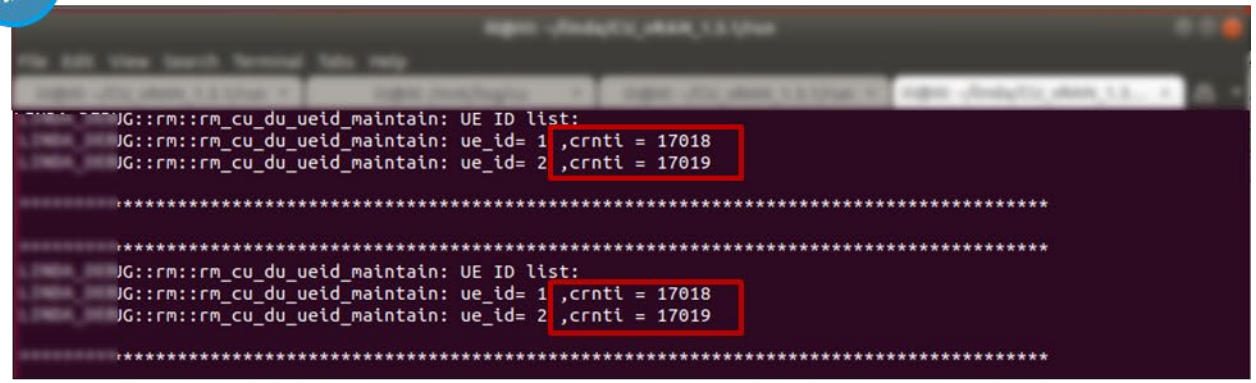
【技術自主性範例2】印出過渡的參數並檢查是否正確

- ORAN 架構下，CU端印出C-RNTI參數



前 無C-RNTI資訊

後 定時印出UEID及C-RNTI資訊



謝謝聆聽，歡迎會後交流